CERT

Preventing Insider Sabotage: Lessons Learned From Actual Attacks

Dawn Cappelli

November 14, 2005

Software Engineering Institute

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **14 NOV 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**
4. TITLE AND SUBTITLE **Preventing Insider Sabotage: Lessons Learned From Actual Attacks**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**39**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Agenda

What is CERT?

Are Insiders a Threat?

CERT/U.S. Secret Service (USSS) Insider Threat Study

Best practices

- Supporting Findings
- Case Examples

What's Next

Questions/Discussion

# What is CERT?

Center of Internet security expertise

Established in 1988 by the Department of Defense (DARPA) in 1988 on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Located in the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

CERT

Security Information Flow

The CERT/CC gains a broad view of Internet security threats with data from many sources. CERT/CC analysts synthesize the data and publish timely, accurate information fast. Researchers develop long-term strategies to improve system security and survivability.
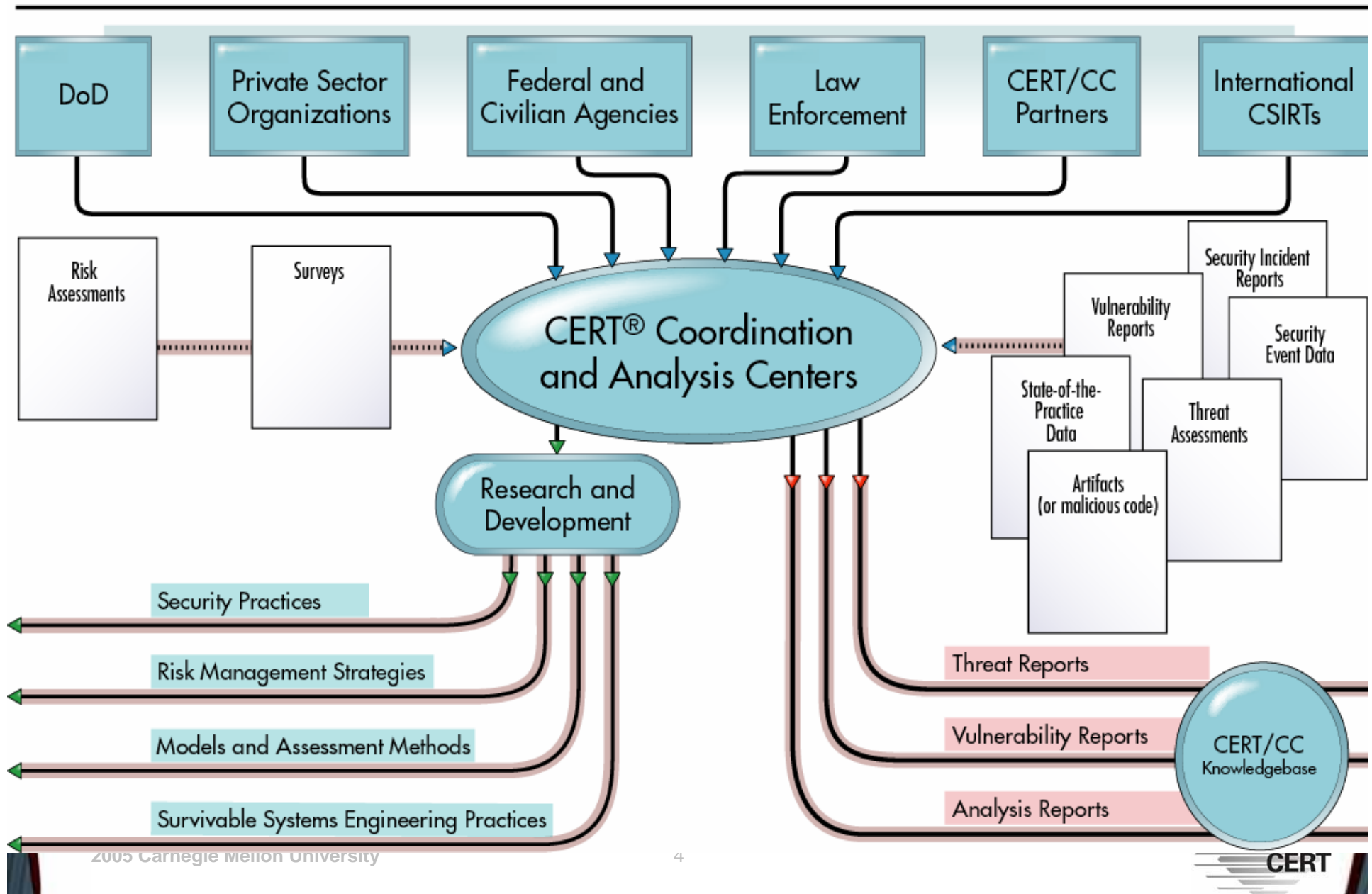
CERT

Are Insiders a Threat?

CERT

e-Crime Watch

CSO, USSS & CERT/CC

819 respondents

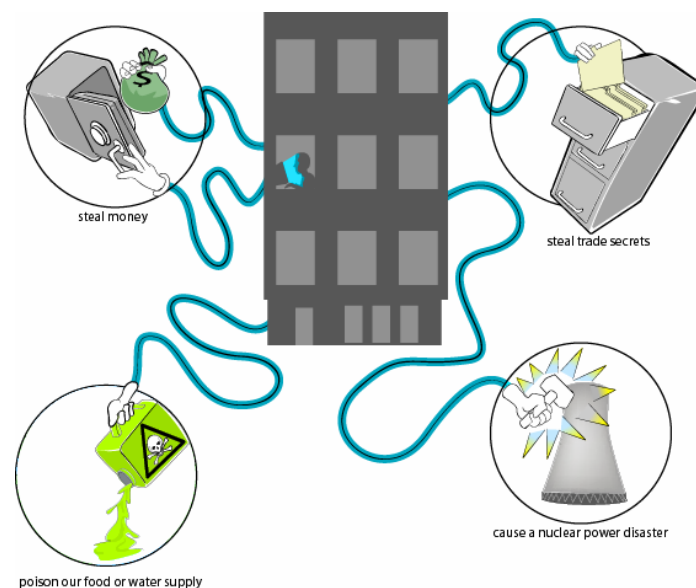Average number of e-crimes in 2004: 86

35% increase in e–crimes in 2004

68% at least one e-crime or intrusion

39% of the organizations experienced one or more insider attacks or intrusions

20% of all attacks by insiders (versus outsiders)

CERT

"*We'are all too paranoid, no point looking behind your back, we are already here.*"

Posted by: Anonymous

CERT

"idiocy to say the least
having been a statistic myself
i see that fear and stupidy prevail
nothing is secure
trust no-one
ever"

Posted by: C0rpR4t3_H4C|<

CERT

USSS/CERT Insider Threat Study

Definition of insider

Purpose of the study

Study method

Reports

Study Definition of Insider

Current or former employees or contractors who

- intentionally exceeded or misused an authorized level of access to networks, systems or data in a manner that

- targeted a specific individual or affected the security of the organization's data, systems and/or daily business operations

CERT

Study Purpose

Identify information that was known or potentially detectable prior to the incident.

Analyze physical, social and online behaviors of insiders.

Develop information to help private industry, government and law enforcement better understand, detect and prevent harmful insider activity.

CERT

Study Method

Incidents perpetrated by insiders in critical infrastructure sectors.

Initial incidents occurred between 1996 and 2002.

Reported publicly or investigated by the Secret Service.

Reviewed primary source material (investigative reports, court documents) and conducted supplemental interviews.

CERT

USSS/CERT Insider Threat Study

Definition of insider

Purpose of the study

Study method

Reports
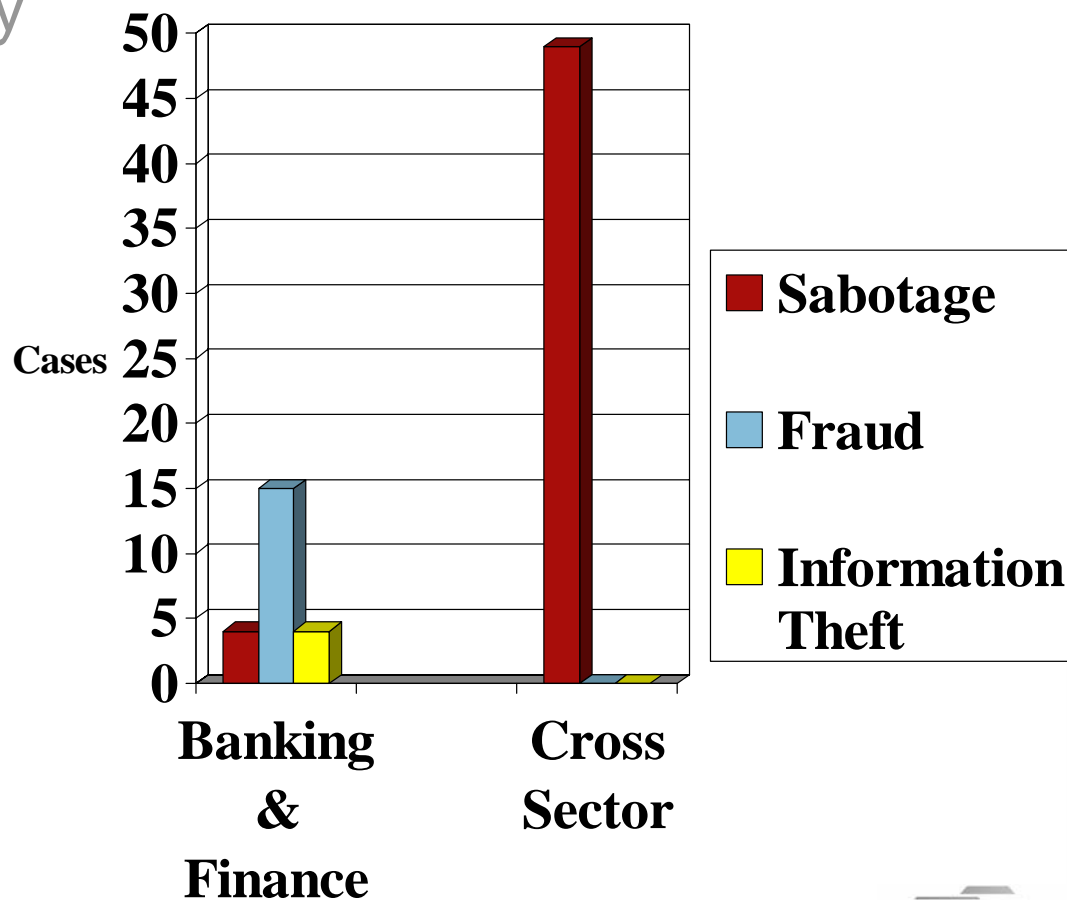
Insider Sabotage
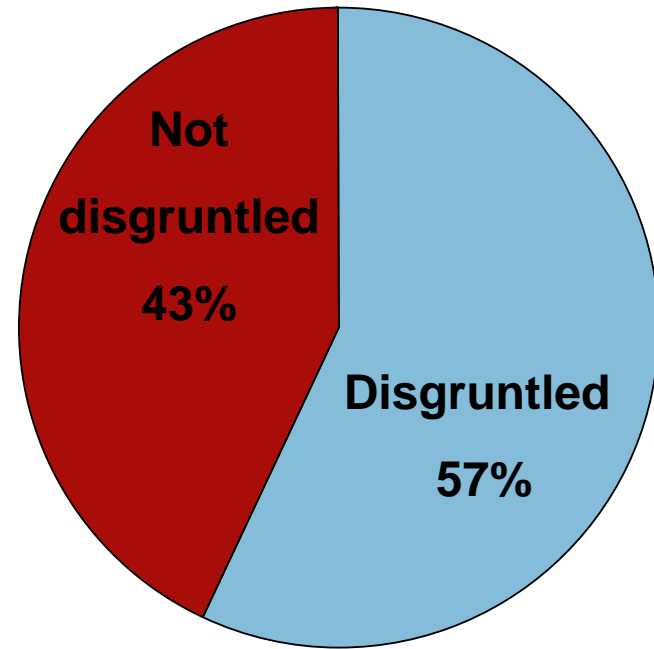
Who were they?

Why did they do it?

What were the
consequences?

Best practices

- Supporting Findings
- Case Examples

Insider Threat

CERT

Who Were the Insiders?

- Male
- 17-60 years old
- About half married
- Variety of racial & ethnic backgrounds

Not disgruntled 43%

Disgruntled 57%

CERT

Primary Motive

Percentage vs Sabotage Cases

- Financial
- Revenge
- Response to negative event

84% Revenge, 92% Response to negative event

CERT
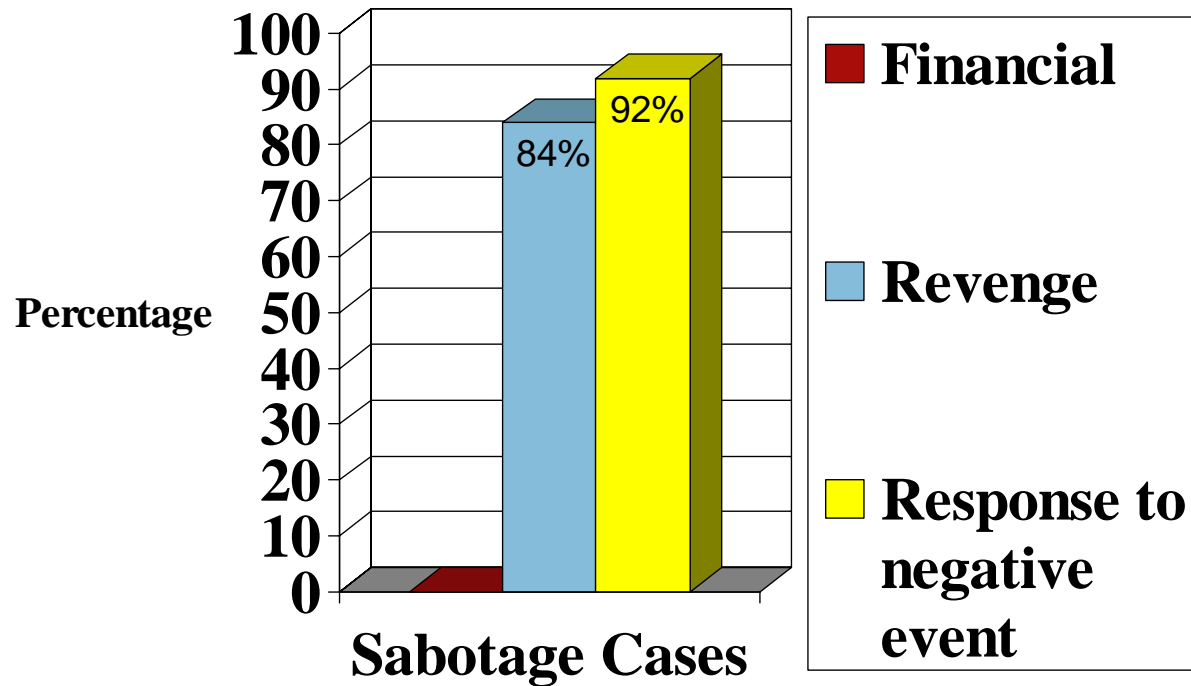
Consequences to Targeted Organizations

Financial Loss

Harm to Individuals
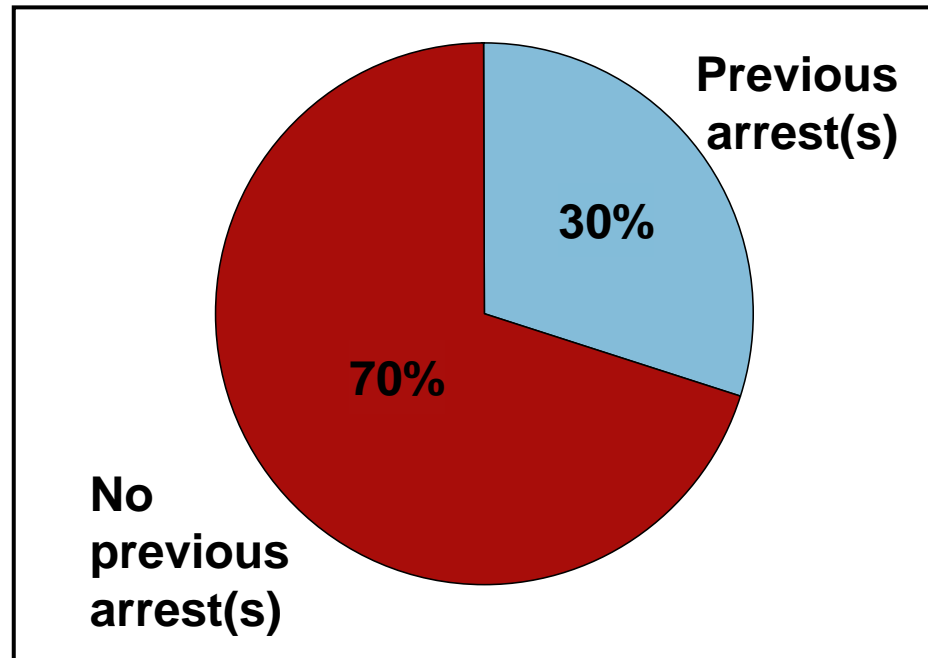
Consequences to Targeted Organizations

Financial Loss

Harm to Individuals

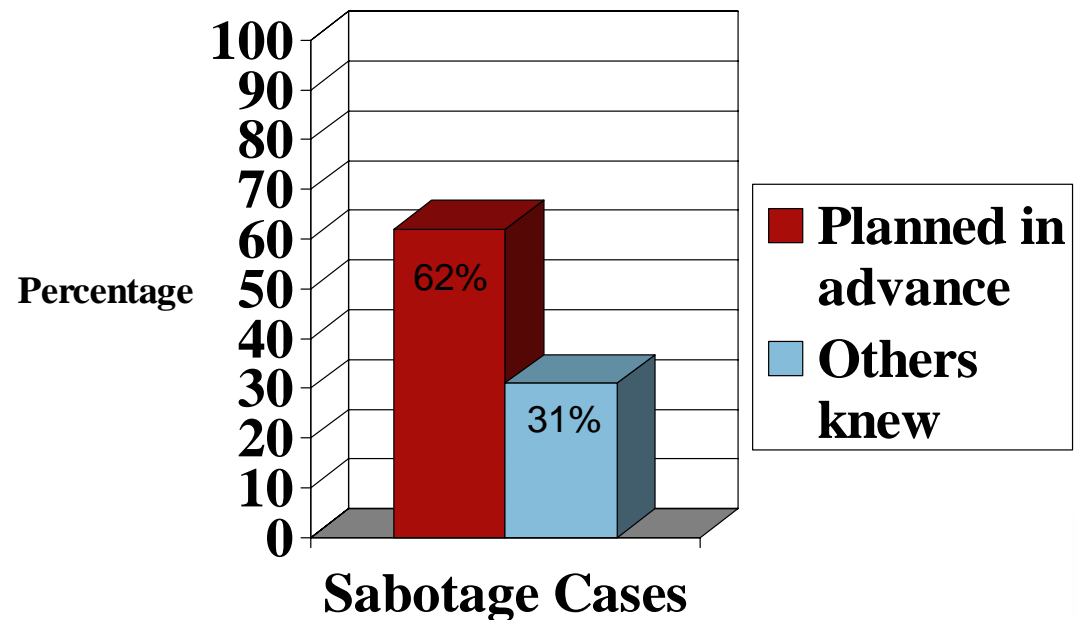Pie chart: Harmed an individual 35%, No individual harm 65%

CERT

Best Practices

CERT
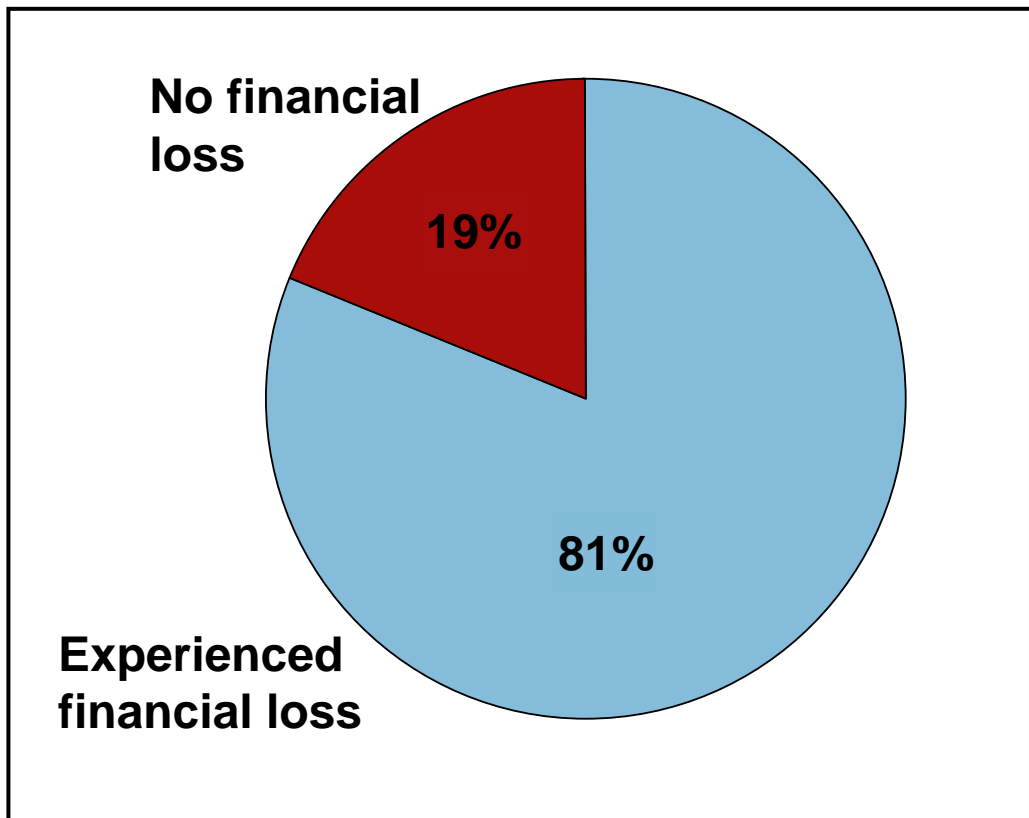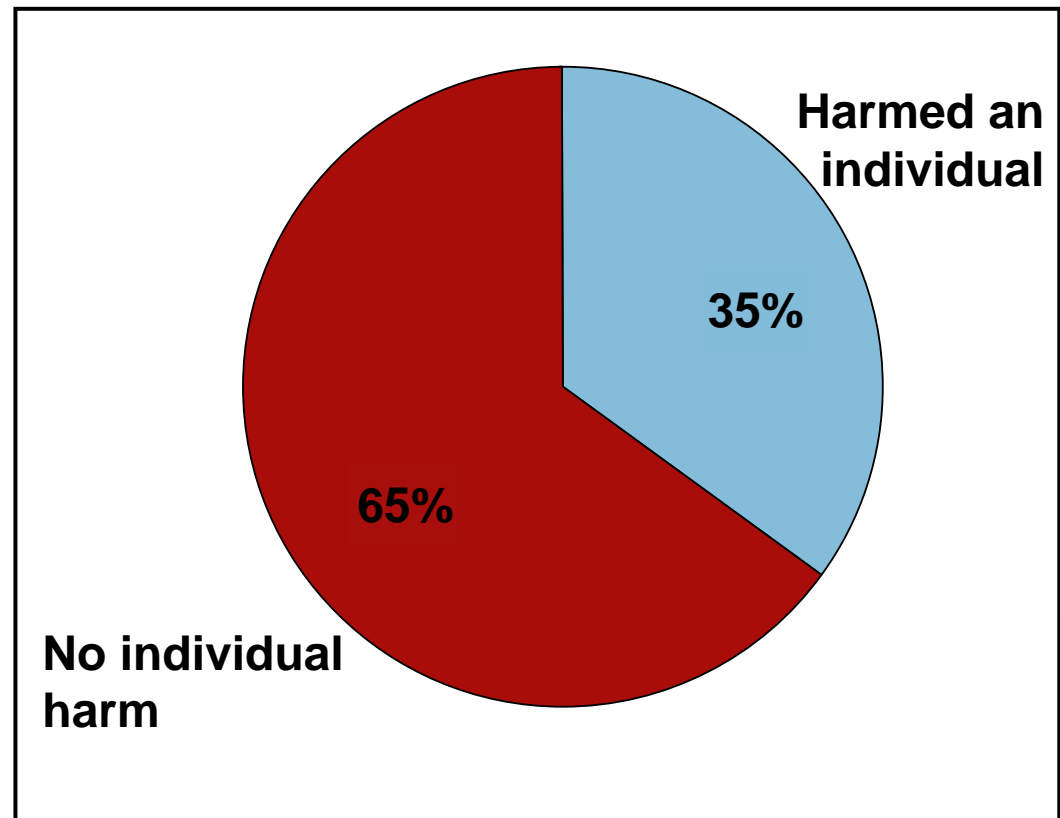
Background checks

Conduct background checks & consider results carefully.

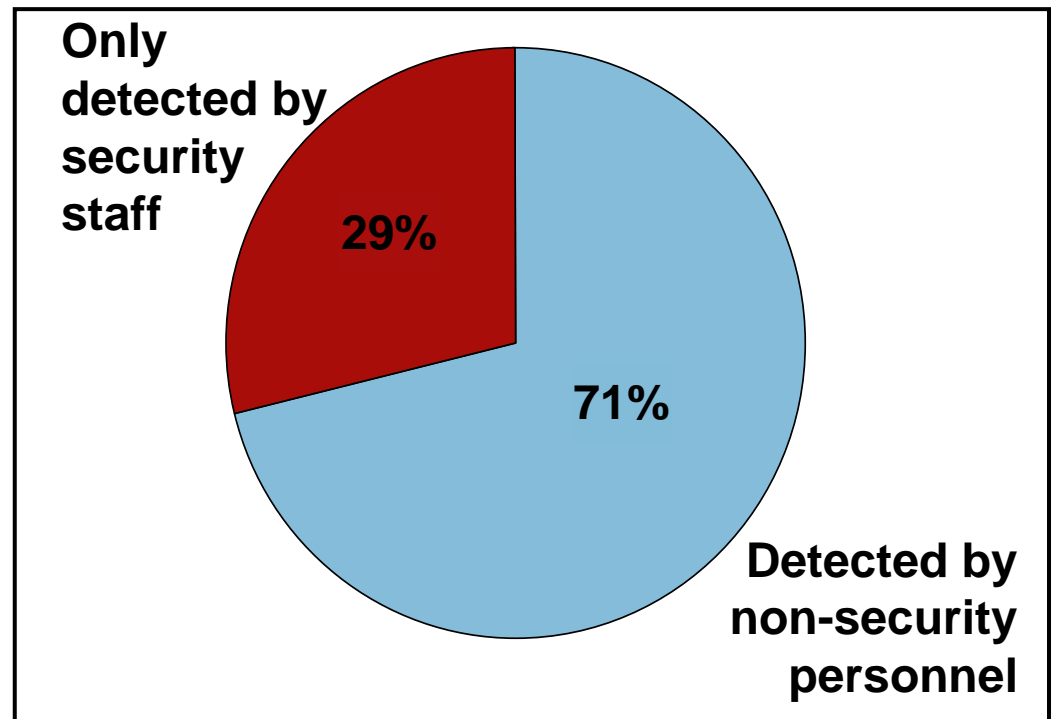Previous arrest(s) 30%

No previous arrest(s) 70%

Security Awareness Training

Institute periodic employee security awareness training for all employees.

Separation of Duties
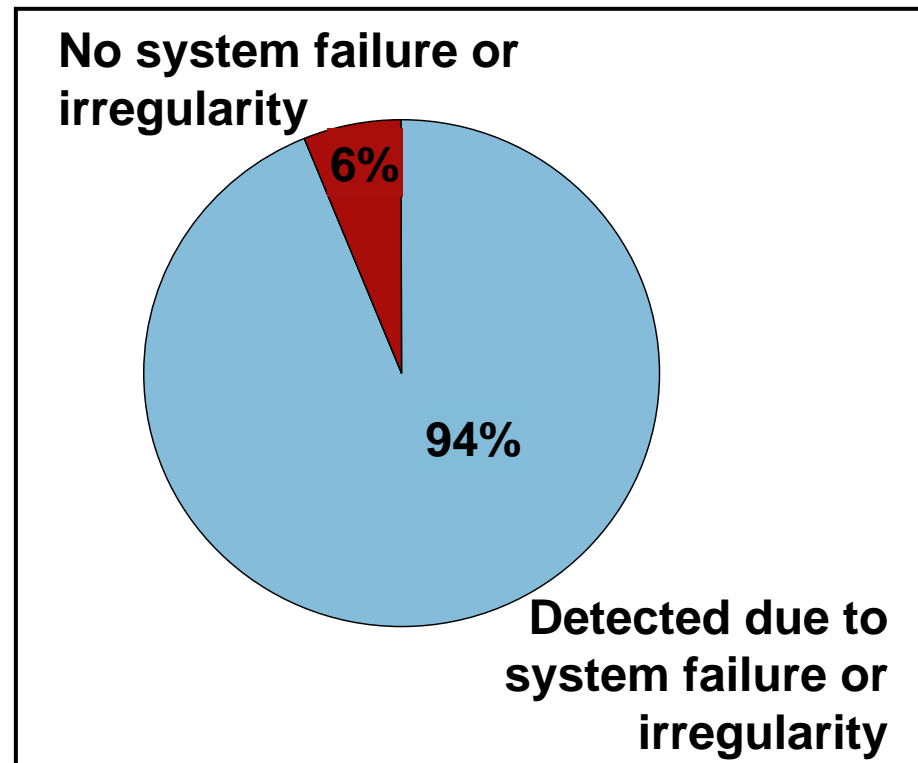
Enforce separation of duties and least privilege.

Only detected by security staff

29%

71%

Detected by non-security personnel

CERT

Password & Account Management

Implement strict password and account management policies and practices.

Had authorized access — 43%

Did not have authorized access — 57%

CERT
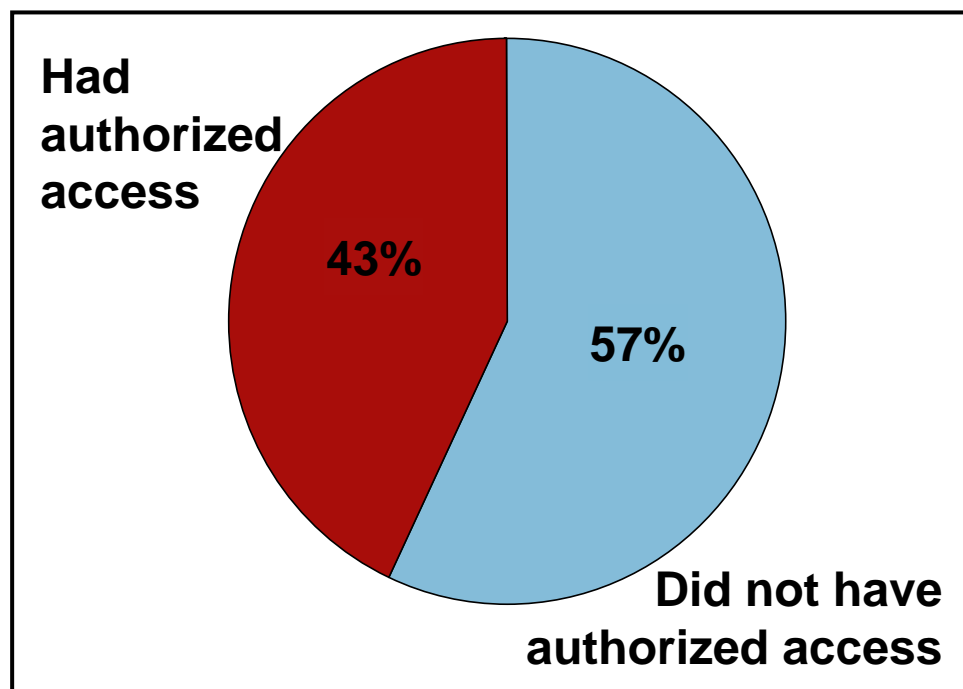
Monitoring

Log, monitor, and audit employee online actions.

No system failure or irregularity

6%

94%

Detected due to system failure or irregularity
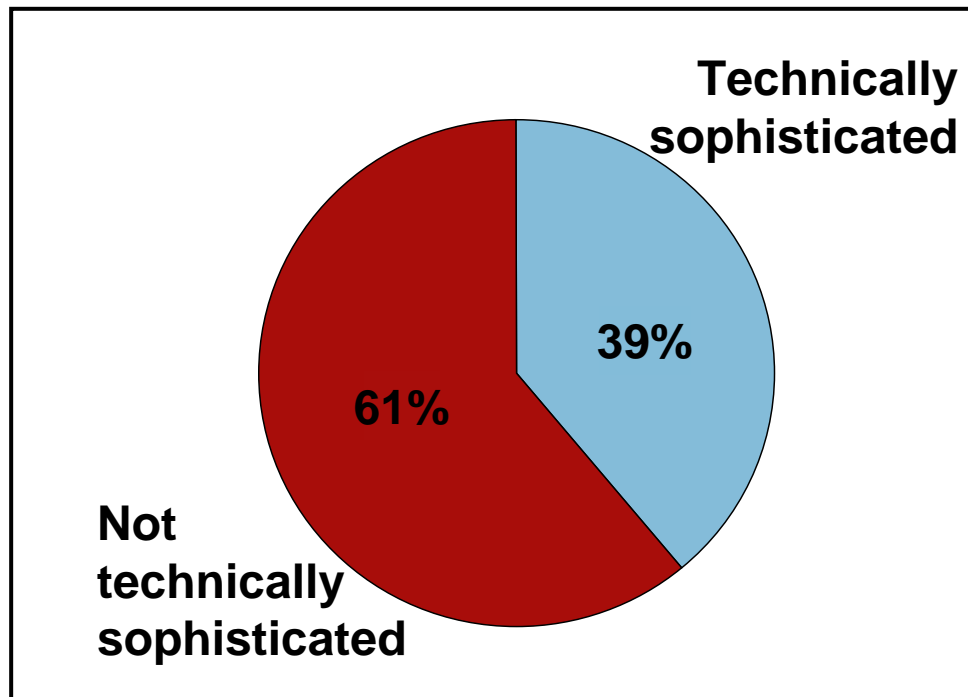
CERT

System Administrators

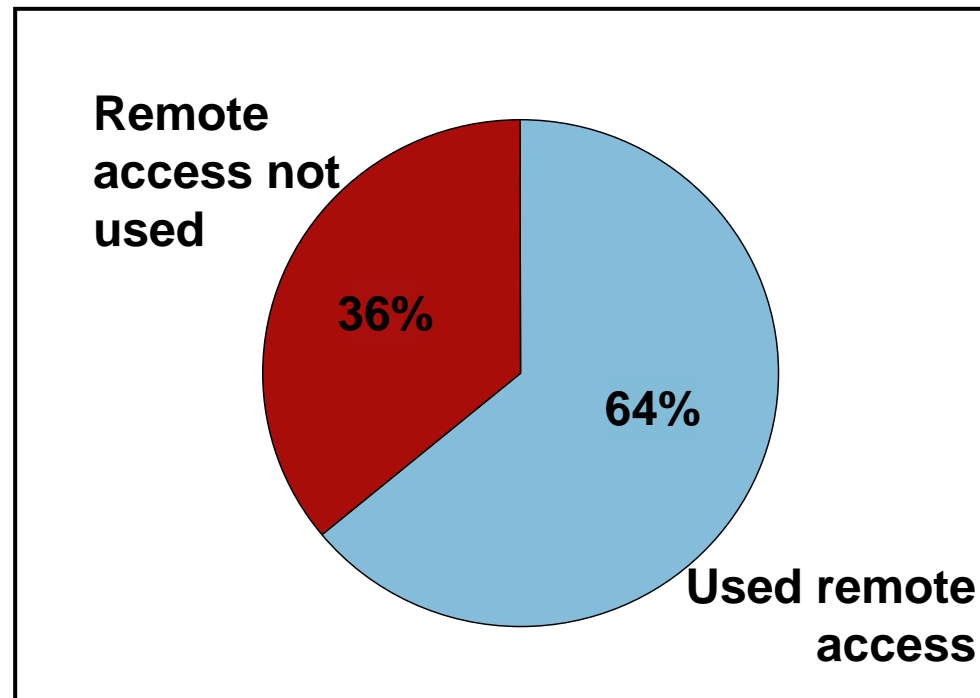*Use additional controls
for system administrators
and privileged users.*
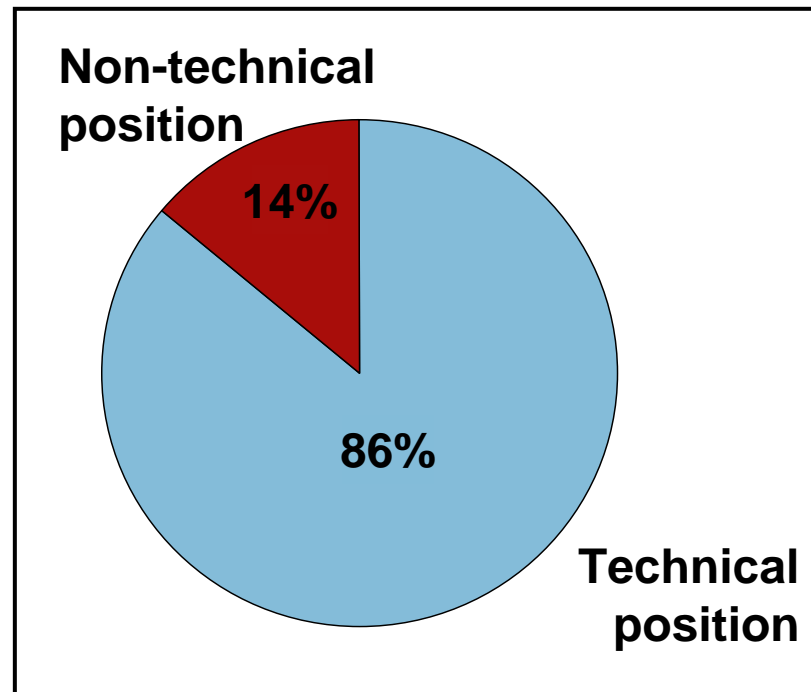
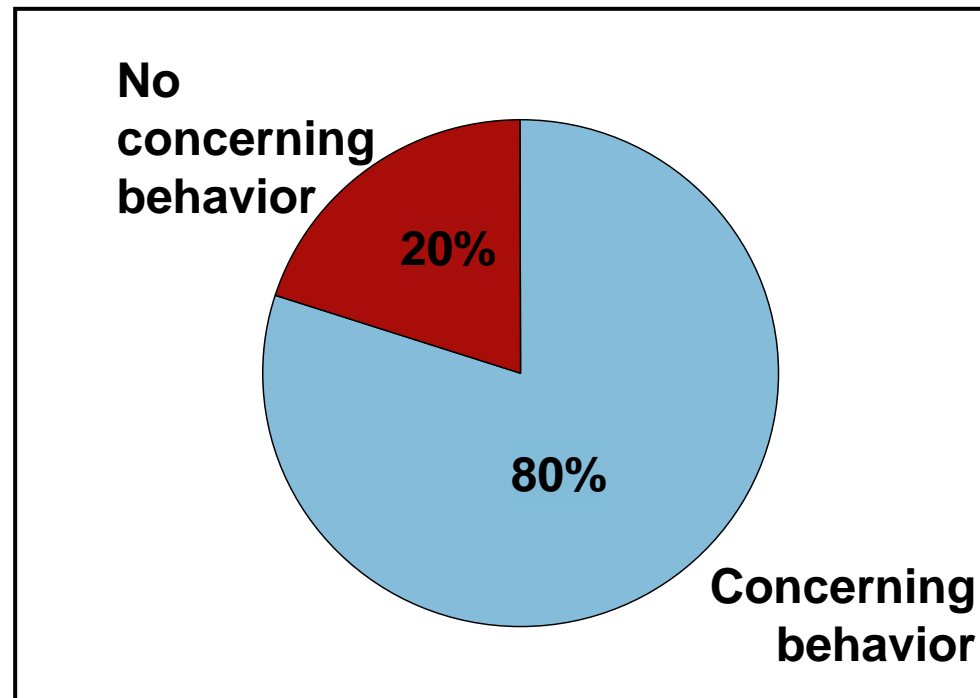# Malicious Code

Actively defend against malicious code.

Remote Access

Use layered defense against remote attacks.
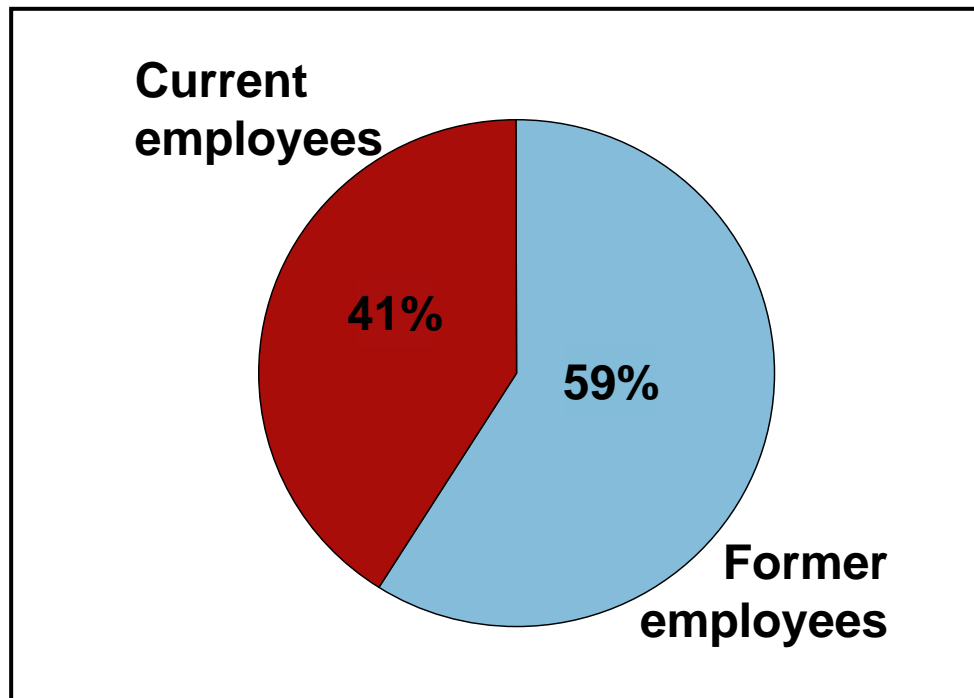

Remote access not used — 36%

Used remote access — 64%

CERT

Suspicious Behavior

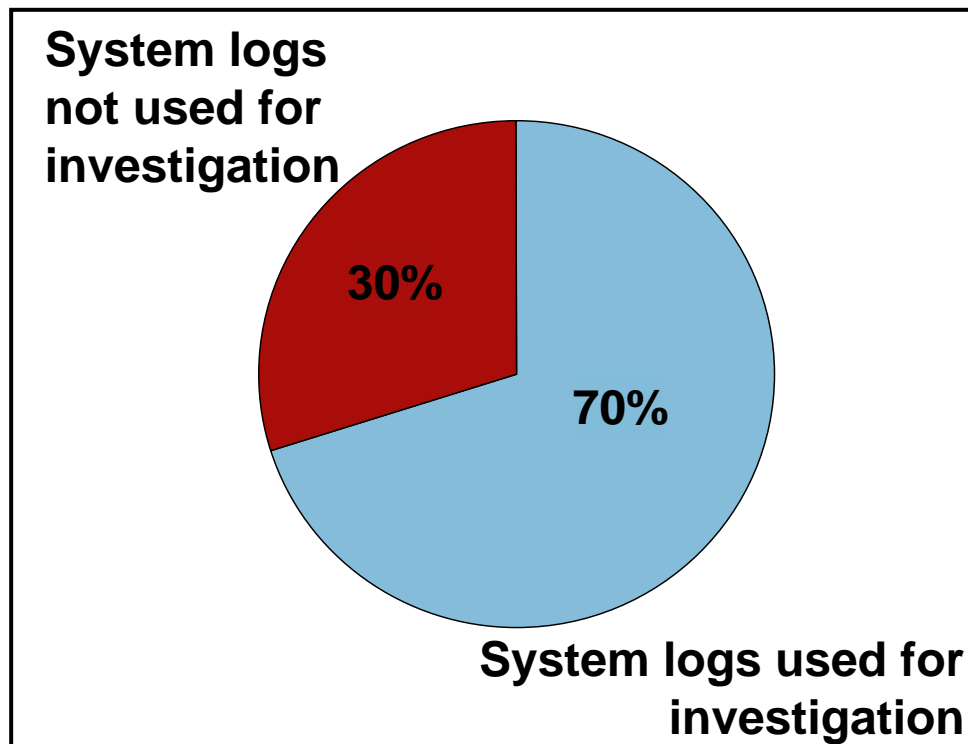*Monitor and respond to suspicious or disruptive behavior.*

CERT

Access Following Termination

*Deactivate access
following termination.*

CERT

Investigation

Collect and save data for use in investigations.

System logs not used for investigation

30%

70%

System logs used for investigation

Back Up & Recovery

Implement secure backup and recovery processes.

No impact on business operations

25%

75%

Impacted business operations

CERT
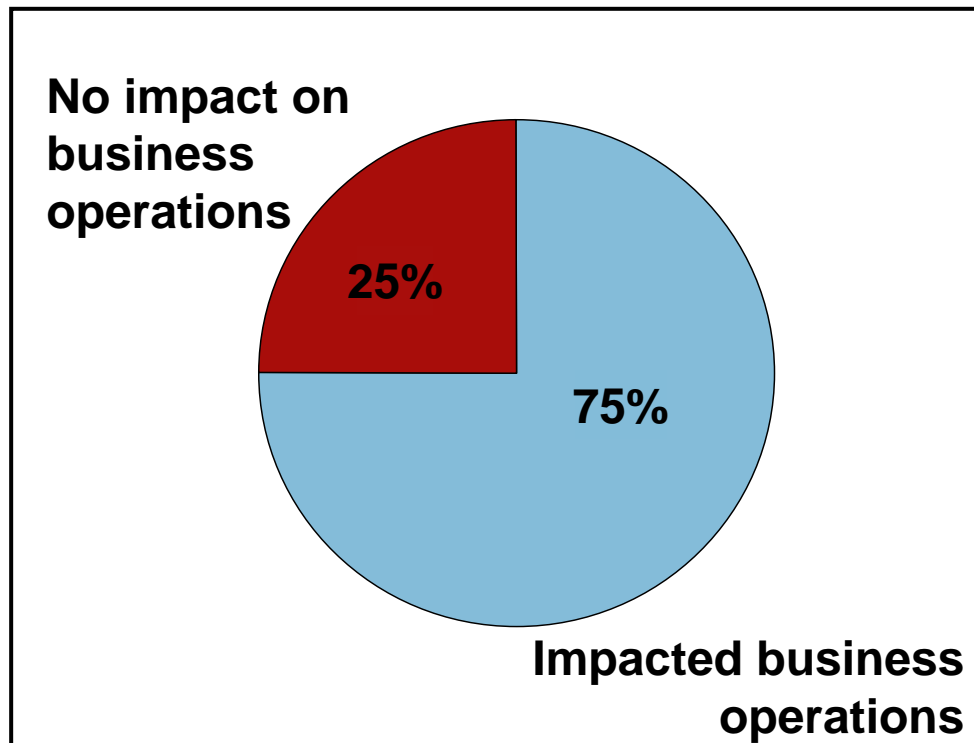
Formal Documentation

Clearly document insider threat controls.

"*Most ITs I know, even the entry-level guys, install root kits as a first order of business when they join a company. They do it as a reflex, not because they have malicious intent or plan to hack the company, but to give themselves convenient access so they can work from home or school.*"

Posted by: Ben |

CERT

Summary of Best Practices

Conduct background checks & consider results carefully.

Institute periodic employee security awareness training for all employees.

Enforce separation of duties and least privilege.

Implement strict password and account management policies and practices.

Log, monitor, and audit employee online actions.

Use additional controls for system administrators and privileged users.

Actively defend against malicious code.

Use layered defense against remote attacks.

Monitor and respond to suspicious or disruptive behavior.

Deactivate access following termination.

Collect and save data for use in investigations.

Implement secure backup and recovery processes.

Clearly document insider threat controls.

CERT

What's Next

In progress:

- Additional "sector reports"
    - IT sector
    - Government sector
- Training – U.S. Secret Service Electronic Crimes Task Force meetings
- System Dynamics Modeling

Planned:

- Insider Threat Phase 2

CERT

System Dynamics Modeling

Model interaction over time between

- organizational culture

- organization's mission

- policies & procedures

- technology

- behavioral psychology

CERT

MERIT

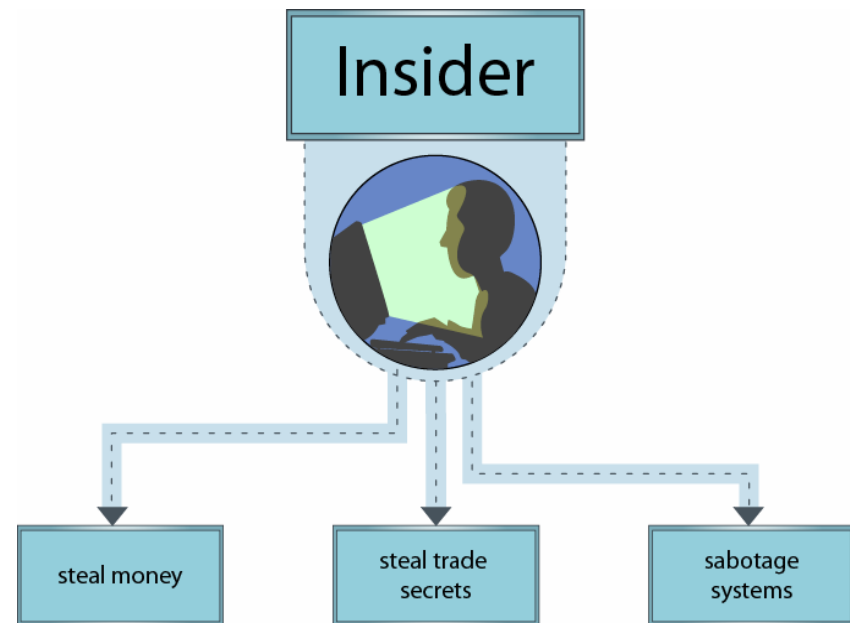## Management Education on Risk of Insider Threat

Management Simulator for insider threat problem

Decision support system for management

Evaluate relative insider threat risk

Insider Threat Phase 2

Collaborate with
government and industry
partners

"I worked at a medium-sized software company, and had root access to their main servers. Purely as an intellectual exercise, I thought about how I could most malliciously use that access. This is what I came up with:

> *Step 1: Hack the backup system: all backups are secretly encrypted as they are made, and decrypted when read back (so that checks of the backups shows nothing.)*

> *Step 2: Wait a year or more.*

> *Step 3: Wipe all the disks on the servers - including the hacked backup encryption/decryption software.*

> *Step 4: Send extortion demand for the encryption key to the backups. Unless they pay, they've lost years of work.*

Of course, I didn't actually try it, so I don't know if it would work..."

Posted by: Filias Cupio

CERT

Questions/Discussion

CERT